STRATEGY RESEARCH PROJECT

INFORMATION ASSURANCE: A NATIONAL POLICY STRUGGLING WITH IMPLEMENTATION

BY

COLONEL ALLEN F. WOODHOUSE
United States Army

USAWC CLASS OF 2001

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

INFORMATION ASSURANCE: A NATIONAL POLICY STRUGGLING WITH IMPLEMENTATION

by

COLONEL ALLEN F. WOODHOUSE
Army

DR. Steven Metz
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Allen F. Woodhouse

TITLE: Information Assurance: A National Policy Struggling with Implementation.

FORMAT: Strategy Research Project

DATE: 10 April 2001 PAGES: 26 CLASSIFICATION: Unclassified

The President's Commission on Critical Infrastructure Protection was the first national effort to address the vulnerabilities created by the revolution in information technology. The Commission was established in July 1996 and rendered its report in October 1997. The results of the report were alarming. The nation's critical infrastructures had become increasingly automated, inter-linked, and relied heavily on computer controlled systems. Moreover, the Commission found a wide spectrum of threats, increasing vulnerabilities in both private sector and government systems, and no national focus or policy.

After reviewing the report, President Clinton issued Presidential Decision Directive 63 (PDD 63), which became the national policy for Critical Infrastructure Protection, and Information Assurance.

This paper will examine the adequacy and effectiveness of PDD 63. It will focus on how clearly the policy states objectives and acceptable risks. It will address the policy's consistency with the National Security Strategy. Since more than 90 percent of the information systems that the government uses belong to the private sector, the paper will examine the private sector's role in the policy's implementation. Finally, with the current trend toward economic globalization, the issue of foreign policy cooperation must be addressed as well.

TABLE OF CONTENTS

INFORMATION ASSURANCE: A NATIONAL POLICY STRUGGLING WITH IMPLEMENTATION

The information age has ushered in a revolution in technology that has changed lives around the world, and the United States enjoys a comfortable lead in technology development[1]. More than any other nation, the United States is reliant on computer-based technology and information systems. Almost every dimension of our society depends on some type of computer-based system. Whether national security, economic trade and stability, education or entertainment, we rely on one or more elaborate computer driven systems. Even the most mundane tasks such as turning on the lights or buying a loaf of bread is computer controlled, and this trend will continue in the future.[2] While the advancements in technology offer considerable promise for America, they carry within them peril. "All computer-driven systems are vulnerable to intrusion and destruction".[3]

The President's Commission on Critical Infrastructure Protection (PCCIP) was the first national effort to address the vulnerabilities created by the revolution in information technology. The Commission was established in July 1996 and rendered its report in October 1997. The results of the report were alarming. All of the nation's critical infrastructures had become increasingly automated, inter-linked, and relied heavily on computer controlled systems. Moreover, the Commission found a wide spectrum of threats, increasing vulnerabilities in both private sector and government systems, and no national focus or policy.

After reviewing the report, President Clinton issued Presidential Decision Directive 63 (PDD 63) that became the national policy for Critical Infrastructure Protection. PDD 63 is the closest thing there is to a national policy on that part of Information Warfare that has become known as Information Assurance.

This paper will examine the adequacy and effectiveness of PDD 63. It will focus on how clearly the policy states objectives and acceptable risks. It will address the policy's consistency with the National Security Strategy. Since more than 90 percent of the information systems that the government uses belong to the private sector, this paper will examine the private sector's role in the policy's implementation. Finally, with the current trend toward economic globalization, the issue of foreign policy cooperation will be addressed as well.

BACKGROUND:

Critical infrastructures are physical and automated computer based systems that provide services, which are so vital that, if destroyed or incapacitated it could have a catastrophic affect

on the economic security and defense of the United States. The PCCIP identified and defined eight categories of critical infrastructures.

1. Information and Communication – computing and telecommunications equipment, software, processes, and people that support the processing, storage, and transmission of data and information.
2. Electrical Power Systems – the generation stations, transmission and distribution networks that create and supply electricity.
3. Gas and Oil Production, Storage and Transportation - the production and holding facilities for natural gas; crude and refined petroleum.
4. Banking and Finance – the retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems. Associated operational organizations, government operations, and support entities, which are involved in all manner of monetary transactions.
5. Transportation – the nation's physical distribution system critical to supporting the national security and economic wellbeing of this nation.
6. Water Supply Systems – the sources of water, reservoirs and holding facilities, aqueducts and other transport systems.
7. Emergency Services – the medical, police, fire, and rescue systems and personnel, Federal, state and local.
8. Government Services – sufficient capabilities at the Federal, state and local levels of government are required to meet the needs for essential services to the public.

The systems that control these critical infrastructures are increasingly software driven and can be accessed remotely via the Internet. These systems could be attacked from a distance via radio waves or international communications networks, with no physical intrusion beyond an adversary's borders.[4] Examples of some of the attacks that could occur are: A logic bomb or another intrusion device could be placed into rail or airplane computer systems that might cause trains and airplanes to be misrouted and or crash; Intruders might steal or disclose confidential personal, medical, or financial information to blackmail, extort, or cause wide-spread social disruption or embarrassment; and a trap door could be hidden in the code controlling switching centers of the Public Switched Network, or a power grid causing failure on command.[5]

The Internet is a non-secure worldwide communications system linking thousands of computer networks and millions of computers.[6] The computers are owned and operated by foreign and domestic governments at all levels, educational and research institutions, commercial and private sector businesses, corporations, financial institutions, service providers,

and any private citizen who can afford to buy a computer and connect to the Internet. Permitting the critical infrastructures to be connected to the Internet is efficient and cost effective because it allows many geographically dispersed systems to be controlled, monitored, managed, and in some cases repaired from one location anywhere in the world. However, since anyone with a computer and access to the Internet may be able to disrupt proper functioning or destroy the nation's critical infrastructures, the risks for efficiency and cost effectiveness is enormous.

The President's Commission on Critical Infrastructure Protection made recommendations focused in five major areas.

1. Development of a broad program of awareness and education.
2. Conduct infrastructure protection through industry cooperation and information sharing.
3. Consider modifying existing laws related to infrastructure protection.
4. Develop a revised program of research and development.
5. Establish a national structure for management and implementation.

THE PRESIDENT'S POLICY:

PDD 63 set some very ambitious goals with specific dates. The national goal set by President Clinton was a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increased security for government systems by the year 2000.[7] The President intended government to be a model for the private sector. To achieve increased security for government systems by 2000, PDD 63 made every Federal department and agency's Chief Information Officer (CIO) responsible for information assurance. The President's policy also required the CIO to appoint a Critical Infrastructure Assurance Officer (CIAO) to be responsible for protecting all other aspects of the department's critical infrastructures.[8] The CIO may be dual hatted as the CIAO at the department's discretion. The CIOs and CIAOs of every department and agency were given six months to develop a plan for protecting its critical infrastructure.

Attempting to make the Federal Government a model in computer and information systems security is commendable, but seems a bit naïve. First, it failed to recognize the limited technical expertise in the area of information security within the Federal Government. The majority of the nation's information security professionals work in the private sector, and it is extremely difficult for government to compete with the salary industry pays. That is one of the reasons that the Federal Government tends to out source a lot of its more technical projects.

Additionally, practically all of the systems that the government uses were developed by the private sector. And, in most cases the infrastructures that the departments and agencies are expected to protect are owned and operated by private industry for the Federal Government.

Procedurally the Federal Government can do a lot to put prudent practices in place to affect improved security. However, practically all of the critical infrastructures are connected in some way to the Internet and requires private sector intervention and cooperation to provide effective technological security solutions. It is almost impossible for the Federal Government to unilaterally provide effective security for these systems when the vast majority of them belong to the private sector. And even if it could be done the solutions would only last as long as it takes intruders to find ways around them. An example of that can be drawn from the current issue surrounding the Napster web site where music can be downloaded and copied for free. In anticipation of the music industry winning a lawsuit to stop that activity, those who are determined to cheat the system have already posted instructions on the web detailing how to work around the security that will be put in place to prevent further pirating of copyrighted material.

The policy calls for the elimination of "any significant vulnerability to both physical and cyber attacks on the nation's critical infrastructures, including especially cyber systems".[9] That implies an expectation that every system associated with our critical infrastructures can be protected from any significant threat. Although only eight critical infrastructure areas were identified, there are hundreds of systems supporting the operations and maintenance of those infrastructures. I believe that it is impractical to think that we can protect them all. And "if perfect protection could be achieved, it would require constant vigilance at all organizational levels, from top to bottom".[10] A more reasonable and effective approach would be to identify all systems affecting the nation's critical infrastructures, and determine an acceptable level of risk for each system. Then develop criteria that can be used to establish a priority list to tighten security on those systems that need it the most.

PDD 63 also states that the Federal Government will:

1. Immediately establish a national center to warn of and respond to attacks.
2. Develop a detailed plan to protect and defend America against cyber disruptions.
3. Build the capability to protect critical infrastructures from intentional acts by 2003.
4. Seek voluntary participation of private industry to meet common goals for protecting critical systems through public/private partnership.
5. Protect privacy rights and seek to utilize market forces.
6. Seek full participation and input from Congress.[11]

To accomplish those tasks the President's policy created a new government structure to manage and implement information assurance policy and programs. PDD 63 established a National Coordinator whose scope includes foreign terrorism and threats of domestic mass destruction as well as critical infrastructure protection.[12] A National Infrastructure Protection Center (NIPC) was created under the supervision of the Federal Bureau of Investigation (FBI). The NIPC serves as a threat assessment center, focusing on Indications and warnings, vulnerabilities, law enforcement, and coordinating the Federal Government response to incidents.[13] It is the principal organization that is supposed to interface and share information with the private sector. It is expected to foster a positive information sharing relationship with the private sector while maintaining the traditional investigative and secrecy roles of the FBI. Without the private sector's support, protection of the nation's critical infrastructures is virtually impossible and there is evidence that the dual role-played by the FBI is causing concern among some within the private sector.[14] For example, a civilian governmental expert made the following observation during a 1998 seminar strategy game jointly sponsored by the U.S. Army War College and two private sector companies: "Most critical infrastructure industry representatives regard their reaching out to government (including federal law enforcement), as adding little or no value, or as legal problems to be avoided -- at least until the situation the company was experiencing became clearer to the firm's executives".[15]

Not only are some members of the private sector skeptical of the NIPC because of its traditional closed source, proprietary products, and lack of total disclosure mode of operations, they question the NIPC's technical competence as the nation's guardian of cyberspace and critical infrastructures. After more than two years in existence, the NIPC continues to release incomplete and sometimes inaccurate alert messages to the information security community. For example, in late 1999 the NIPC published the wrong technical information on how to identify systems compromised by the RingZero Trojan.[16] The NIPC provided one set of transfer control protocols ports for the Trojan and a number of private sector firms provided another. The Trojan was found living on the transfer control protocol ports provided by the private sector.[17] Additionally, like many government departments and agencies the NIPC contracts out a lot of its technical work. A contract clause by an NIPC vendor prevented the source code of an NIPC malicious code detector from being released to the security community for review.[18] That created a significant setback to the partnership and information sharing initiative between government and the private sector that PDD 63 intended to establish.

The NIPC was also tasked to develop a Key Asset Initiative (KIA), which is designed to identify all computer-based systems involved in the provisioning of the nation's critical

infrastructures. Once the assets are identified the NPIC works with federal, state, and local officials to determine which systems should be designated as "key systems". A recent statement by a FBI Agent tasked with NIPC responsibilities to develop the KIA within the jurisdiction of his FBI Field Office indicates that the FBI lacks the technical expertise and resources to effectively accomplish this task. Apparently he is a one-man show with limited technical training in the eight areas of critical infrastructures, and his office lacks sufficient automation equipment required to manage the program. For almost three years the NIPC has had the important role of collecting and disseminating information from all relevant sources, as well as the development of a comprehensive, indications and warning system. Since an Internet year is approximately three months, a considerable amount of time has been lost already. Moreover, it seems unlikely that much will change in the near term unless the NIPC gets increased funding to hire a technical staff and purchase equipment, or outsource the mission.

PDD 63 also established a Critical Infrastructure Assurance Office to assist the National Coordinator in working with government agencies and the private sector to develop the "National Plan". The National Infrastructure Assurance Council (NIAC) consist of information technology leaders from the private sector, and state and local officials who come together to provide guidance for the formulation of policy for the National Plan.[19] For each infrastructure sector the new governmental structure assigns a single Federal Agency to serve as the Lead Federal Agency to that sector for liaison. The Lead Federal Agency and its private sector counterpart are supposed to work together to develop and implement a vulnerability awareness and education program for their sector.

The infrastructure sectors and their lead federal agencies are:

Infrastructure Sector	**Lead Federal Agency**
Banking and Finance	Department of Treasury
Transportation	Department of Transportation
Electric, Gas & Oil Pipelines	Department of Energy
Information/Communications	Department of Commerce
Government Services	General Services Administration
Fire/Other Emergency Services	Federal Emergency Management Agency
Public Health Services	Dept of Health & Human Services
Water Supplies	Environmental Protection Agency

Also, the new governmental structure identified four special functions related to critical infrastructure protection that must be performed primarily by the Federal Government.[20] Each

special function has a corresponding Lead Federal Agency responsible for coordinating all of the activities of the United States Government in that area. Those special functions and lead agencies are:

Special Functions	Lead Federal Agency
Law Enforcement/Internal Security	Department of Justice
National Defense	Department of Defense
Intelligence	Central Intelligence Agency
Foreign Affairs	Department of State

While the sector assignment of Federal Agencies seems logical and offer an opportunity for dialogue, I question the need for it as well as the establishment of a new organizational structure. First, government moves slowly, and creating more layers of bureaucracy will only exacerbate the problem. There are already concerns about government being too big. Second, the vast majority of the expense for resources (to include personnel) must come from the private sector because they own most of the critical infrastructures. From a policy standpoint government should have the lead. However, the private sector must shoulder the financial burden for most of the resources required to provide the protection needed. Third, some if not most of the functions that these new organizations are created to perform are being conducted to some degree by government agencies that currently exist.

For example, the National Communication System's (NCS) mission is to assist the President, the National Security Council, the Office of Science and Technology Policy, and the Office of Management and Budget in the exercise of their wartime and non-wartime emergency telecommunications functions, and their planning and oversight responsibilities.[21] Additionally, the NCS assist in the coordination of planning for and the provisioning of national security and emergency preparedness telecommunications for the Federal Government under all circumstances, including crises or emergency, attack, recovery, and reconstitution.[22] President Kennedy created the NCS in 1963 after he experienced problems with communications during the Cuban Missile Crises in October 1962. The NCS is composed of twenty- three federal departments and agencies that include Department of Defense, Department of State, Department of Justice, the Joint Staff, the National Security Agency and Central Intelligence-Agency. Many of the agencies tasked with new responsibilities under PDD 63 are members of the NCS. Also, the NCS provides administrative support to the President's National Security Telecommunications Advisory Committee (NSTAC), and it is the focal point for joint industry/government planning.

The NSTAC was established in 1982 to provide advice and expertise to the President on issues and problems related to national security and emergency preparedness telecommunications policy.[23] It consists of up to thirty of the nation's major telecommunications related industries within the private sector. The NSTAC members are the Chief Operating Officers and Presidents of corporations such as GTE, AT&T, BankAmerica, Sprint and Hughes Corporations. Some of the activities that the NSTAC is involved with are: electronic commerce, cyber security, widespread Internet outage, and infrastructure assurance.

The NCS and NSTAC have developed a close partnership and is a model for government/private sector cooperation and information sharing. In fact they work side by side daily at the National Coordinating Center for Telecommunications (NCC) which is located at the NCS. The NCC is an industry/government organization that assists in the initiation, coordination, restoration, and reconstitution of national security and emergency preparedness telecommunications services and facilities. Although the NCS and NSTAC focus is on telecommunication systems, the technical expertise and government/private sector partnership required to achieve the goals of PDD 63 are available and mature within these two existing organizations. Certainly their practices can be adopted to fit the requirements of the other seven critical infrastructure sectors.

ROLE OF THE PRIVATE SECTOR:

The public switched telephone network, the electric power grids, and most of the systems that make up the global information infrastructure and the Internet are private sector assets. Recognizing that the private sector is really the owner of the vast majority of the nation's critical infrastructures, PDD 63 seeks a close partnership between government and the private sector. Government desires this relationship in hope that private companies will share information about attacks on and vulnerabilities of their systems to better defend them and reduce vulnerabilities. Critical to the success of establishing and sustaining a close partnership is developing a trusting relationship. Although both government and the private sector have a significant incentive to protect critical infrastructures, their interest, concerns, and expectations vary. For example, the government is motivated primarily by national and economic security concerns.[24] However, while the private sector is concerned about security of its networks, it is driven by business concerns and profits.[25] To stay in business the private sector must be concerned about attacks from competitors, insider abuse, protecting investor interests, and providing customers with a safe, secure, and private means of conducting electronic commerce.[26]

Having different interest can lead to different views of the threats, vulnerabilities, and level of acceptable risks. From a law enforcement perspective, government might want to identify and publicly prosecute someone accused of cyber-crime even if the accused is a corporate insider. However, the negative publicity resulting from such a trial might tarnish the affected company's reputation. Exposing vulnerabilities and the fact that its systems were exploited is the kind of publicity that may cause a corporation's investors and customers to lose confidence and discontinue their business relationship with them. Additionally, proprietary information or confidential business material that a private firm might share with government in good faith might be subject to release under the Freedom of Information ACT (FOIA). On the other hand, for national security reasons, the government may be reluctant to share classified information that may help the private sector deter or prevent electronic intrusions. Moreover, it takes time for the government to declassify classified material, which could jeopardize time sensitive operations.

In spite of the different interest and concerns between government and the private sector in terms of critical infrastructure protection, the private sector is where the critical infrastructure is. The ultimate financial responsibility for protecting them belongs to the private sector as well. And government cannot unilaterally provide for the protection of these systems. Moreover, the companies responsible for almost all critical infrastructure systems have already developed significant risks analyses and contingency plans to respond to denial of service and outages.[27] Unfortunately, the level of risk these companies are comfortable with may not be suitable for national security purposes. Therefore, it is imperative that government and the private sector establish a partnership rooted in trust that ensures that sharing of information is equitable, protected, and beneficial to the interest of both parties. Although much progress has been made, the current dialogue involves reluctance on both sides to full disclosure. Clearly adequate protection of these critical systems will not happen without private sector cooperation, considering their ownership. To ensure that relationship is established, I believe the responsibility lies with government to find ways to promote private sector cooperation. Government can start by removing the barriers (whether actual or perceived) that prevent full private sector cooperation such as the fear of compromising proprietary information under the FOIA or otherwise. Nevertheless, volumes can be learned from the relationship between the NCS and NSTAC. They should serve as a model for the cooperation between government and industry that PDD 63 seeks.

FOREIGN POLICY ISSUES:

A major shortfall of PDD 63 is that it primarily seeks to protect domestic systems while the trend is clearly toward economic globalization. The policy and the National Plan that was developed to implement the policy acknowledge the international implications of the Global Information Infrastructure (GII), but focuses on domestic issues. The Internet is a complex, dynamic world of interconnected networks with no clear boundaries and no central control. Within the U.S. law enforcement personnel can conduct electronic surveillance, subpoena records, issue search warrants, and seize evidence when a crime is committed. Overseas U.S. law enforcement officials must depend on the local authorities for assistance, and a viable foreign policy on cyber crime will make their jobs much easier.[28]

As we have seen in previous cyber attacks, intruders disguise their actual location by spoofing or going through several sites before attacking their objective. The sites used may be in several different countries. The situation can be further complicated by an intrusion that occurs within the borders of the United States but routed through Internet Service Providers and computer networks of several foreign countries. By the time law enforcement officials can successfully trace the attack the intruder may be gone. Even an investigation of an attack within the U.S. using domestic service and systems may take quite some time if the perpetrator goes through several states before attacking a system. Successful investigations of cyber crimes depend on a more timely response than a traditional international case, because electronic evidence can be lost completely if not secured quickly.

To the NIPC's credit it has begun a dialogue with several countries to address the issue of cooperation in cyber crime incidents. The FBI has international partners that they routinely work with in their traditional law enforcement role. They have wisely expanded that role as their mission expanded with the establishment of the NIPC. However, the NIPC cannot make U.S. policy and is therefore limited to the cooperation their foreign contacts are willing to provide. Nevertheless, their initiative on this front is commendable.

THE NATIONAL SECURITY STRATEGY:

The national security strategy (NSS) published for President Clinton in December 1999 by the National Security Council, recognized the protection of the nation's critical infrastructures as a "vital interest". An entire section of the strategy is devoted to critical infrastructure protection. Within that section the strategy acknowledge that "other governments and terrorist groups are creating sophisticated, well organized capabilities to launch cyber attacks against critical American information networks and the infrastructures that depend on them".[29] The strategy

clearly articulates the basic tenets of PDD 63. It lists the critical infrastructures and the threat. It identifies the requirement to establish a partnership between the Federal Government and private industry. The NSS states that the U.S. will develop intrusion detection technology and the capability to rapidly restore service to systems in the face of serious attack.[30] Additionally, the strategy recognizes the lack of a trained and qualified pool of security personnel. Finally, the NSS practically quotes PDD 63 when it states that the U.S. is increasing information security research and development, and developing a plan (the National Plan) to defend our critical infrastructures.[31]

Although not specifically mentioned in the critical infrastructure protection section of the strategy, the need to pursue international cooperation to protect the nation's critical systems is recognized in several areas throughout the document as it speaks to "shaping the international security environment".[32] The only inconsistency between the national security strategy and PDD 63 is that PDD 63 calls for an initial operational capability to protect critical infrastructures by May 2000, and the national security strategy extends that requirement until May 2001. In spite of the extension, both documents expect to achieve full operational capability by the year 2003.

OBSERVATIONS:

PDD 63 is a significant and positive step in the right direction to guard against the threats to the nation's critical infrastructures. It is well written, clear in its intentions, and addresses the issues that need to be worked and resolved to provide better protection. However, several obstacles must be overcome to achieve real progress.

First, it is impractical to think that every system associated with the survivability and availability of the nation's critical infrastructures can be protected. Clearly what is needed is a prioritized list of what exactly is to be protected. The NIPC should be given authority to task those agencies (such as energy, transportation, etc) with critical infrastructure expertise to assists in the development of the key asset initiative. It is clearly beyond the NIPC's technical capability to accomplish it alone. Developing a realistic prioritized list of what is to be protected is the first step in this process now that the threats have been identified. PDD 63 recognize this but does not adequately address how to achieve it.

The President's policy does an excellent job of stating the need for a partnership with the private sector. However, to date neither side can or will deliver in a manner that the other deems adequate".[33] This relationship is critical because the private sector and government are

inextricably tied together on this problem.[34] This remains a sticking point for the success of the National Plan.

Another challenge for success of the National Plan is achieving the international cooperation required. While the state department and other agencies tasked to secure international cooperation, success among those countries not friendly with the United States seems unlikely. Additionally, the focus of PDD 63 is primarily on domestic concerns. However, it recognizes that domestic and international issues in this arena cannot be separated.[35] While this appears to be a significant foreign policy challenge, there is so much still to do at home that there may be little the U.S. can influence abroad.

PDD 63 talks about the Federal Government acting first to secure its networks and being a model for the private sector. Much has been done in DoD with the active role of its Computer Emergency Response Teams (CERT), and JTF-CND, and its concept of "defense in depth" (multi-layered defenses using firewalls, encryption, digital signatures etc). However, there is much evidence that there are still major vulnerabilities throughout the Federal Government. A September 2000 General Services Administration (GAO) report revealed that since July 1999 Federal computer security continues to be fraught with weaknesses, and the range of individual agencies weaknesses has broadened.[36] It stated for example, weaknesses in the Department of Treasury increase the risk of fraud associated with billions of dollars of federal payments and collections, and weaknesses in DoD increased the vulnerability of various military operations that supports the department's war-fighting capability.[37] It also stated that "further information security weaknesses places enormous amounts of confidential data at risk of inappropriate disclosure".[38] The data at risk ranges from personal tax data to proprietary business information. Not only does the results of the report demonstrate the Federal Government's failure to be a role model in information security, it severely hurts the partnership it seeks to build with the private sector.

CONCLUSION:

Much remains to be done to protect the nation's critical infrastructures. The milestone of achieving true protection of all critical infrastructures by 2003 is extremely ambitious and I believe unattainable. In fact, there are still questions as to whether the Bush administration will continue to pursue the goals laid out in PDD 63. Certainly modifications are needed particularly in terms of identifying exactly what must be protected and how much risk is acceptable. The formidable challenge of overcoming the obstacles in building a government/private sector partnership must be given top priority. The example of the relationship between the NCS and

the NSTAC should be explored not only for building a trusted partnership, but to prevent any duplication of effort from the new structure that has been established. Finally, the State Department must do more to assist the NIPC in furthering the nation's foreign policy dialogue.

WORD COUNT = 4892

ENDNOTES

[1] Jeffrey A. Hunker,""CIAO: AN INTERGRATED APPROACH TO COUNTER THREATS OF A "NEW ERE" , An interview with Dr. Jeffrey A. Hunker, Director of the Critical Infrastructure Assurance Office,"" U.S. Foreign Policy Agenda, November 1998, interviewed by the U.S. Information Agency: available from<http://usinfo.state.gov/journals/itps/1198/1jpe/pj48hun.htm>; Internet; accessed 9 December 2000.

[2] William J. Clinton, "National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue, the President's Message. " 7 January 2000: available from<http://www.ciao.gov/National_Plan/NationalPlanActivities.htm> Internet; accessed 8 September 2000.

[3] Ibid.

[4] Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law. (Washington, D.C.: National Defense University, 1997), 3.

[5] Ibid. 3-5

[6] Elizabeth S. Lane and Craig Summerhill, Internet primer for information professionals: a basic guide to Internet networking technology (Westport, CT: Meckler, 1993), 1.

[7] White Paper, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," May 1998; available from<http://www.ciao.gov/CIAO_Document_Library/paper598.html>; Internet; accessed 8 September 2000.

[8] Ibid.

[9] Ibid.

[10] William Gravell, ""SOME OBSERVATIONS ALONG THE ROAD TO "NATIONAL INFORMATION POWER," ""available from<http://www.law.duke.edu/journals/djcil/articles/dcil9p401.htm>; Internet; accessed 21 September 2000.

[11] White Paper.

[12] "FACT SHEET: PROTECTING AMERICA'S CRITICAL INFRASTRUCTURES," (Presidential Decision Directive 63), 22 May 1998; available from<http://usinfo.state.gov/journals/itps/1198/ijpe/pj48wpfx.htm>; Internet accessed 29 December 2000.

[13] Ibid.

[14] Gravell.

[15] Ibid.

[16] Richard Forno, "NIPC – A Failure To Communicate", 2 September 2000; available from <http://www.iwar.org.uk/cip/resources/nipc/2000-06.html>; Internet accessed 31 December 2000.

[17] Ibid.

[18] Ibid.

[19] "FACT SHEET: PROTECTING AMERICA'S CRITICAL INFRASTRUCTURES."

[20] White Paper.

[21]"United States", Joint Chiefs of Staff, Joint Staff; Information Assurance: legal, Regulatory, Policy and Organizational Considerations, 4th ed.(Washington D.C.: August 1999), B-19

[22] Ibid.

[23] Ibid, B-29.

[24] Jack Brock, "Congressional Testimony before the Subcommittee on Government Management, Information, and Technology," 26 July 2000; available from <http://www.house.gov/reform/gmit/hearings/2000hearings/000726cybersec.../000726jb.ht>; Internet; accessed 1 October 2000.

[25] Ibid.

[26] Dan Woolley, Congressional Testimony before the Subcommittee on Government Management, Information, and Technology," 22 July 2000; available from <http://www.house.gov/reform/gmit/hearings/2000hearings/000622.hr4042/000622dw.htm>; Internet> accessed 11 September 2000.

[27] Roger C. Molander, "Congressional Testimony before the Subcommittee on Government Management, Information, and Technology," 26 July 2000; available from <http://www.house.gov/reform/gmit/hearings/2000hearings/000726cyberse.../000726rm.ht>; Internet; accessed 1 October 2000.

[28] Michael A. Vatis, "Congressional Testimony before the Subcommittee on Government Management, Information, and Technology," 26 July 2000; available from <http://www.house.gov/reform/gmit/hearings/2000hearings/000726cybersecurity/000726mv.htm >; Internet; accessed 9 September 2000.

[29] William J. Clinton, A National Security Strategy for a New Century (Washington, D.C.: The White House, October 1999), 17.

[30] Ibid,18.

[31] Ibid.

[32] Ibid,5.

[33] Molander.

[34] Winn Schwartau, "Infrastructure Is Us," (Feature U.S. Infrastructure Protection), June 1999; available from <http://www.infosecuritymag.com/jun99/Infrastruc.htm>; Internet: accessed 29 December 2000.

[35] Gravell.

[36] General Accounting Office, Information Security: Report to Congressional Requesters (Washington, D.C.: U.S. General Accounting Office, September 2000), 2.

[37] Ibid.

[38] Ibid.

BIBLIOGRAPHY

Brock, Jack. "Congressional Testimony before the Subcommittee on Government Management, Information, and Technology." 26 July 2000. Available from <http://www.house.gov/reform/gmit/hearings/2000hearings/000726cybersec.../000726jb.ht>; Internet. Accessed 1 October 2000.

Clinton, William J. A National Security Strategy for a New Century Washington, D.C.: The White House, October 1999.

_____. "National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue, the President's Message." 7 January 2000. Available from<http://www.ciao.gov/National_Plan/NationalPlanActivities.htm>. Internet. Accessed 8 September 2000.

FACT SHEET: "Protecting America's Critical Infrastructures." Presidential Decision Directive 63. 22 May 1998. Available from<http://usinfo.state.gov/journals/itps/1198/ijpe/pj48wpfx.htm>. Internet Accessed 29 December 2000.

Forno, Richard. "NIPC – A Failure To Communicate". 2 September 2000. Available from <http://www.iwar.org.uk/cip/resources/nipc/2000-06.html>. Internet Accessed 31 December 2000.

General Accounting Office. Information Security: Report to Congressional Requesters. Washington, D.C.: U.S. General Accounting Office. September 2000.

Gravell. William. ""Some Observations Along the Road to "National Information Power"."" Available from<http://www.law.duke.edu/journals/djcil/articles/dcil9p401.htm>. Internet. Accessed 21 September 2000.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. Information Warfare and International Law. Washington, D.C.: National Defense University, 1997.

Hunker, Jeffrey A.""CIAO: An Integrated Approach to Counter Threats of A "New Ere". An interview with Dr. Jeffrey A. Hunker, Director of the Critical Infrastructure Assurance Office,"" U.S. Foreign Policy Agenda.. Interviewed by the U.S. Information Agency. November 1998. Available from<http://usinfo.state.gov/journals/itps/1198/1jpe/pj48hun.htm>. Internet. Accessed 9 December 2000.

Lane, Elizabeth S., and Craig Summerhill. Internet Primer for Information Professionals: A Basic Guide to Internet Networking Technology. Westport, CT: Meckler, 1993.

Libicki, Martin C. "Defending Cyberspace and other Metaphors". Washington, D.C.: National Defense University, 1997.

_____. "What is Information Warfare". Washington, D.C.: National Defense University, 1995.

Molander, Roger C. "Congressional Testimony before the Subcommittee on Government Management, Information, and Technology". 26 July 2000. Available from <http://www.house.gov/reform/gmit/hearings/2000hearings/000726cyberse.../000726rm.ht>. Internet. Accessed 1 October 2000.

Molander, Roger C., Peter A. Wilson, David A. Mussington, and Richard F. Mesic. Strategic Information Warfare Rising. Washington D.C.: National Defense Research Institute, 1998.

Schwartau, Winn. "Infrastructure Is Us". Feature U.S. Infrastructure Protection. June 1999. Available from <http://www.infosecuritymag.com/jun99/Infrastruc.htm>. Internet. Accessed 29 December 2000.

Shalikashvili, John M. National Military Strategy of the United States of America. Washington, D.C.: 1997.

_____.Information Warfare, A Strategy for Peace...The Decisive Edge in War. Washington, D.C.:1996.

United States. Joint Chiefs of Staff, Joint Staff. Information Assurance: legal, Regulatory, Policy and Organizational Considerations, 4th ed. Washington, D.C.: August 1999

_____.Information Assurance through Defense in Depth. Washington, D.C.: February 2000.

Vatis, Michael A. "Congressional Testimony before the Subcommittee on Government Management, Information, and Technology". 26 July 2000. Available from <http://www.house.gov/reform/gmit/hearings/2000hearings/000726cybersecurity/000726mv.htm >. Internet. Accessed 9 September 2000.

White Paper, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63". May 1998. Available from<http://www.ciao.gov/CIAO_Document_Library/paper598.html>. Internet; Accessed 8 September 2000.

Woolley, Dan. Congressional Testimony before the Subcommittee on Government Management, Information, and Technology." 22 July 2000. Available from <http://www.house.gov/reform/gmit/hearings/2000hearings/000622.hr4042/000622dw.htm;Inter net>. Accessed 11 September 2000.